

CLAIMS

1. Apparatus (10) for generating an encrypted data stream
from an audio and/or video signal, comprising:
5
an encoder (16) for encoding the audio and/or video
signal in order to generate a data stream with a
predefined data stream syntax as output signal;
10
an encryption means (18) coupled with the encoder (16)
for influencing encoder internal data (20a) and/or the
output signal (20b) of the encoder (16) in a uniquely
reversible manner based on a key (k1) such that the
generated encrypted data stream comprises payload
15
information differing from payload information of a
data stream that would be generated by the apparatus
(10) without the presence of the encryption means (18)
and that the generated encrypted data stream comprises
the predefined data stream syntax.
20
2. Apparatus according to claim 1, wherein said
encryption means (18) is further arranged to influence
the encoder internal data (20a) and/or the output data
(20b) of the encoder 16 based on the key such that the
25
encoded data stream has the same bit length as a data
stream that would be generated by said apparatus (10)
without the presence of said encryption means.
3. Apparatus according to one of the previous claims,
30
wherein the encryption means (18) is arranged in order
to influence the encoder internal data (20a) and/or
the output data (20b) of the encoder merely so
strongly based on the key that the payload information
of the encrypted data stream differs only so strongly
35
from the payload information of a data stream that
would be generated without the presence of the
encryption means (18) that a decoder that does not
possess the key provides a decoded output signal based

on the encrypted data with a quality that is lower than the quality that the decoder would provide if he possessed the key, wherein however, a minimum quality is ensured.

5

4. Apparatus according to one of the previous claims, wherein said encryption means (18) is arranged in order to merely influence said encoder internal data (20a).

10

5. Apparatus according to claims 1 to 4, wherein the encoder is an encoder for audio signals, comprising:

15

an analysis filter bank (204) for converting the audio signal from the time domain into a spectral representation in order to obtain spectral values; and

20

a quantizing means (206) for quantizing the spectral values under consideration of a psychoacoustic model (208) that generates quantized spectral values as main information and scale factors as side information each of which is associated to at least one quantized spectral value; and

25

wherein said encryption means (18) is arranged to influence the scale factors generated by said quantizing means (206) based on the key.

30

6. Apparatus according to claims 1 to 4, wherein said encoder is an encoder for audio signals, comprising:

35

an analysis filter bank (204) for converting the audio signal into a spectral representation in order to obtain spectral values; and

a quantizing means (206) for quantizing the spectral values under consideration of a psychoacoustic model (208) that generates quantized spectral values as main

information and scale factors as side information each of which is associated to at least one quantized spectral value; and

- 5 wherein said encryption means (18) is arranged to influence the quantized spectral values generated by said means (206) for quantizing.
- 10 7. Apparatus according to claim 6, wherein said encryption means (18) is arranged to resort the quantized spectral values based on the key.
- 15 8. Apparatus according to claims 6 or 7, wherein said encryption means is arranged to link at least part of the quantized spectral values with a pseudo random bit sequence generated based on the key as start value via an EXCLUSIVE-OR-link.
- 20 9. Apparatus according to claims 6 to 8, wherein merely least significant bits of spectral values are linked with a pseudo random bit sequence.
- 25 10. Apparatus according to claims 6 to 9, wherein said quantized spectral values are signed and wherein said encryption means (18) is arranged to change the signs of quantized spectral values based on the key.
- 30 11. Apparatus according to claims 6 to 10, wherein said encoder (16) further comprises an entropy encoder (210) that is arranged to carry out an entropy encoding of the quantized spectral values via a plurality of predefined code tables.
- 35 12. Apparatus according to claim 11, wherein said entropy encoder (210) is arranged such that it comprises at least one code table which is an unsigned code table such that a sign for a code word from the code table is written separately from the code word into the

payload information, wherein said encryption means (18) is arranged to change the sign of at least one quantized spectral value based on the key before said entropy encoding of said quantized spectral values.

- 5
13. Apparatus according to claims 11 or 12, wherein each code table for the entropy encoding of the quantized spectral value is provided in a certain frequency band with at least one spectral value, wherein at least one frequency band has two or more quantized spectral values and wherein said encryption means (18) is arranged to resort the two or more quantized spectral values in the frequency band having two or more quantized spectral values based on the key.
- 10
14. Apparatus according to claims 11 to 13, wherein at least one code table of the plurality of code tables is a multidimensional code table, wherein a code word represents a plurality of quantized spectral values, wherein said encryption means (18) is arranged to resort groups of quantized spectral values, wherein one group of spectral values has so many quantized spectral values as encoded by a code word of said multidimensional code table.
- 15
15. Apparatus according to claims 1 to 3, wherein the output data of said encoder (16) comprise a sequence of code words, wherein said sequence of code words represents an entropy encoded version of the audio and/or video signal, wherein said encryption means (18) is arranged for influencing the output data (20b) of said encoder in order to resort the sequence of code words based on the key.
- 20
- 25
- 30
- 35 16. Apparatus according to one of the previous claims, wherein said encoder has a plurality of sub-blocks (204 to 210) connected with a bit stream multiplexer (212) multiplexing the data output from the single

sub-blocks according to the predefined data stream syntax in order to obtain the output data of said encoder (16).

- 5 17. Apparatus (70) for generating a data stream encrypted based on a second key (k2) from a first data stream encrypted based on a first key (k1), wherein said first data stream is an audio and/or video signal encoded by using an encoder with a predefined data stream syntax, wherein said first data stream is encrypted such that encoder internal data have been influenced based on the first key (k1), comprising:
- 10

a partial decoder (36') for reversing part of the encoding such that the influenced encoder internal data are present;

15

an decryption means (38) for decrypting the encoder internal data based on the first key (k1);

20

an encryption means (18) for influencing the encoder internal data based on the second key (k2);

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted based on the second key (k2), wherein the second data stream has the predefined data stream syntax.

25

- 30 18. Apparatus (70') for generating a second data stream encrypted based on a key (k1) from a data stream, wherein said first data stream is an audio and/or video signal encoded using an encoder with a predefined data stream syntax, comprising:

35 a partial decoder (36') for reversing part of the encoding such that encoder internal data to be influenced are present;

an encryption means (18) for influencing the encoder internal data based on a key (k1);

5 a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted based on the key (k1), wherein the second data stream has the predefined data stream syntax.

10

19. Apparatus (80) for generating a decrypted data stream from a first data stream encrypted based on a key (k1), wherein said first data stream is an audio and/or video signal with a predefined data stream syntax encoded by using an encoder, wherein said first data stream is encrypted such that encoder internal data has been influenced based on the first key (k1), comprising:

15

20

a partial decoder (36') for reversing part of the encoding such that the influenced encoder internal data are present;

25

a decryption means (38) for decrypting the encoder internal data based on the key (k1);

30

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the second data stream with the predefined data stream syntax.

35

20. Apparatus according to claims 17 to 19, wherein said partial decoder (36') has a bit stream demultiplexer (222), wherein said encoder internal data are the output data from the bit stream demultiplexer (222).

21. Apparatus according to claim 20, wherein said partial decoder (36') further comprises an entropy decoder

(224) following the bit stream demultiplexer (222), wherein said encoder internal data are the output data from the entropy decoder (224).

- 5 22. Apparatus according to claims 17 to 19, wherein said encoder internal data are quantized spectral values and/or scale factors.
- 10 23. Apparatus (30) for generating a decrypted audio and/or video signal from an encrypted data stream representing an audio and/or video signal, wherein the encrypted data stream comprises payload information differing from payload information of a non-encrypted data stream and wherein said encrypted data stream
15 comprises the same data stream syntax as a non-encrypted data stream, comprising:
- 20 a decoder (36) for decoding input data in order to generate decoded output data; and
- 25 a decryption means (38) for influencing the encrypted data stream (40a) and/or of encoder internal data (40b) based on a key in order to reverse the uniquely reversible changes which have been carried out in an apparatus for generating an encrypted data stream in order to obtain the decrypted audio and/or video signal.
- 30 24. Apparatus according to claim 23, wherein said encrypted data stream comprises quantized spectral values which have been influenced by an encryption means; and
- 35 wherein said decryption means (38) is arranged in order to reverse the influencing of the quantized spectral values.

25. Apparatus according to claim 24, wherein said decoder (36) comprises:

5 an entropy decoder (24) for reversing said entropy encoding in order to obtain the influenced quantized spectral values.

26. Apparatus according to claim 24, wherein said decoder (36) further comprises:

10 an entropy decoder (224) for reversing the entropy encoding into which the uninfluenced quantized spectral values can be fed,

15 wherein said encryption means (38) is arranged in order to reverse the influencing of the entropy encoded spectral values.

27. Apparatus (30) according to claims 23 to 26, wherein said decoder further comprises:

20 a plurality of functional blocks coupled with a bit stream demultiplexer (222) conducting parts of the data stream to the single blocks according to the predefined data stream syntax.

28. Apparatus (30) according to claims 23 to 27, wherein said decoder (36) further comprises:

30 a synthesis filter bank (228) in order to convert a spectral representation of the audio and/or video signal into a timely or local representation.

29. Method for generating an encrypted data stream representing an audio and/or video signal, comprising:

35

encoding (16) of an input signal in order to generate an encoded data stream with a predefined data stream syntax as output signal;

5 wherein during the step of encoding and/or after the step of encoding the following step will be carried out:

10 influencing of data during the encoding of encoder internal data (20a) and/or the output signal (20b) in a uniquely reversible manner based on a key, such that the generated encrypted data stream comprises payload information differing from payload information of a data stream that would be generated by the step of
15 encoding without the step of influencing and that the generated encrypted data stream comprises the predefined data stream syntax.

20 30. Method for generating a decrypted data stream from an encrypted data stream representing an audio and/or video signal, wherein said encrypted data stream comprises payload information differing from payload information of a non-encrypted data stream and wherein said encrypted data stream has the same data stream
25 syntax as a non-encrypted data stream, comprising:

decoding (36) of input data in order to obtain decoded output data; and

30 wherein the following step is carried out before the step of decoding and/or during the step of decoding:

35 influencing (38) the input data (40a) and/or the data (40b) during the decoding based on a key used for encoding such that the encrypted data stream will be decrypted.